National Infrastructure Protection Center
CyberNotes

Issue #2001-19 *September 24, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between September 4 and September 21, 2001. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Alessandro Gardich[1]	Unix	nss_ postgresql 0.6.1	A vulnerability exists in the NSS (Name Service Switch) database module, 'nss_postgresql' because SQL queries can be manipulated via an HTTP request, which could let a malicious user obtain access to restricted resources.	No workaround or patch available at time of publishing.	NSS_PostGre SQL Remote SQL Query Manipulation	Medium	Bug discussed in newsgroups and websites.
Apache Group[2]	MacOS X 10.x	Apache 1.3.14Mac	A vulnerability exists when an Apache webserver is used with the Mac OS X client, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	MacOS X Client Apache Directory Contents Disclosure	Medium	Bug discussed in newsgroups and websites.

[1] RUS-CERT Advisory 2001-09:01, September 10, 2001.
[2] Bugtraq, September 10, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apple[3]	MacOS X 10.x	MacOS X 10.0-10.0.4	A vulnerability exists in the programs 'nireport,' 'nidump,' and 'netinfo,' which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Macintosh OS X FBCIndex File Contents Disclosure and .DS_Store Directory Listing Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
Check Point Software[4]	Multiple	Firewall-1 4.0, 4.1, 4.1SP1-SP4	A buffer overflow vulnerability exists in logging of authentication attempts by the GUI log viewing clients, which could let a remote malicious user execute arbitrary code as root.	No workaround or patch available at time of publishing.	Firewall-1 GUI Log Viewer	**High**	Bug discussed in newsgroups and websites.
Check Point Software[5]	Multiple	Firewall-1 3.0, 4.0, 4.1, 4.1SP1	A vulnerability exists due to the creation of predictable /tmp files, which could let a malicious user potentially gain root access.	Upgrade available at: http://www.checkpoint.com/techsupport/downloads/downloads.html	Firewall-1 Policyname Temporary File Creation	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Check Point Software[6]	Multiple	Firewall-1 3.0, 4.0, 4.1, 4.1SP1&SP2	A symbolic link vulnerability exists because Log Viewer will overwrite files ending in the .log extension, which could let a malicious user create and overwrite files on the system and launch a Denial of Service attack.	No workaround or patch available at time of publishing.	Firewall-1 GUI Client Log Viewer Symbolic Link	Low/ Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Computer Associates[7]	Windows NT 4.0/2000	ARCServe 2000 Advanced Edition 7.0, ARCServe 2000, ARCServe 6.61	Two vulnerabilities exist: a vulnerability exists in the default installation because an insecure network share is created, which could let a malicious user obtain sensitive information; and passwords for the administrator account are stored in cleartext, which could let a malicious user gain administrative access.	Patch for the Insecure Default Network Share vulnerability is available at: ftp://ftp.ca.com/CAproducts/unicenter/arcserveitaent/0006/qo00945/QO00945.CA	ARCServe Insecure Default Network Share and Cleartext Administrative Password	Medium/ **High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Counter-pane[8]	Windows 95/98/NT 4.0/2000	Password Safe 1.7.1	A vulnerability exists when the program option to clear passwords from the clipboard is enabled, which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	Password Safe Data Buffer Recovery	Medium	Bug discussed in newsgroups and websites.

[3] Bugtraq, September 10, 2001.
[4] Bugtraq, September 19, 2001.
[5] Bugtraq, September 8, 2001.
[6] Securiteam, September 10, 2001.
[7] Bugtraq, September 16, 2001.
[8] Bugtraq, September 13, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
CrossTec Corp[9]	Windows 95/98/NT 4.0/2000	NetOp School 1.5	A vulnerability exists because all security checks and password dialogs are bypassed, which could let a malicious user gain administrative access without authentication.	No workaround or patch available at time of publishing.	NetOp School Administration Authentication	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Digital (Compaq)[10]	Unix	TRU64/ DIGITAL UNIX 4.0d-4.0g	Two vulnerabilities exist: a vulnerability exists because 'msgchk' fails to check file permissions, which could let a malicious user gain root privileges; and a buffer overflow vulnerability exists in the 'msgchk' utility, which could let a malicious user gain root privileges.	Temporary workaround (Bugtraq): Unless msgchk must be run suid, (i.e., for support of "rpop"), strip the suid bit (chmod u-s /usr/bin/mh/msgchk).	Digital Unix MSGCHK MH_PROFILE Symbolic Link and MSGCHK Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
DLink Technol-ogies[11]	Multiple	D-Link Dl-704 V2.56b5	A Denial of Service vulnerability exists when a malicious user sends a large amount of fragmented IP packets.	Upgrade available at: available: http://www.dlink.com.tw/2000e/download/download.htm	DLink IP Fragment Denial Of Service	Low/**High** **(High if DDoS best-practices not in place)**	Bug discussed in newsgroups and websites. Exploit script has been published.
Eric Raymond [12, 13] ***Conectiva and RedHad release patches***[14, 15]	**Unix**	**Fetchmail 5.8- 58.9**	**Two vulnerabilities exist in both the imap and pop3 code because the input is not verified when used to store a number in an array, which could let a remote malicious user gain access to client systems and execute arbitrary code.**	**Upgrade available at: http://tuxedo.org/~esr/fetchmail/fetchmail-5.8.17.tar.gz** **Debian:** **http://security.debian.org/dists/stable/updates/main/** ***Conectiva:*** ftp://atualizacoes.conectiva.com.br/ ***RedHat:*** ftp://updates.redhat.com/	**IMAP and POP3 Reply Signed Integer Index**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Hassan Consulting[16]	Windows NT 4.0	Shopping Cart 1.23	A vulnerability exists because certain types of user-supplied input are not filtered, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Shopping Cart Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
Hewlett-Packard Company[17]	Unix	HP-UX (VVOS) 11.0.4	A Denial of Service vulnerability exists due to the library function in 'libsecurity'.	Patch available at: PHCO_24852 http://itrc.hp.com	HP-UX VVOS libsecurity Denial of Service	Low	Bug discussed in newsgroups and websites.

[9] Bugtraq, September 11, 2001.
[10] Bugtraq, September 10, 2001.
[11] Fate Research Labs Security Advisory, F8-DLINK20010906, September 6, 2001.
[12] Bugtraq, August 10, 2001.
[13] Debian Security Advisory, DSA-071-1, August 10, 2001.
[14] Conectiva Linux Security Announcement, CLA-2001:419, September 5, 2001.
[15] Red Hat Security Advisory, [RHSA-2001:103-04, September 10, 2001.
[16] Bugtraq, September 8, 2001.
[17] Hewlett-Packard Company Security Bulletin, #0166, September 6, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ian Lance Taylor[18, 19]	Unix	Taylor UUCP 1.0.6	A vulnerability exists due the way configuration files are handled when passed to UUCP via the 'config flag', which could let a malicious user gain elevated privileges and administrative access.	**Caldera:** ftp://ftp.caldera.com/pub/updates/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/	Taylor UUCP Argument Handling Privilege Elevation	High	Bug discussed in newsgroups and websites. Exploit has been published.
IBM[20]	Multiple	Lotus Domino 5.0.8	A vulnerability exists when a specially formed GET request is submitted to the server, which could let a malicious user obtain the server's internal address.	No workaround or patch available at time of publishing.	Lotus Domino Internal IP address Disclosure	Medium	Bug discussed in newsgroups and websites.
IBM[21]	Windows NT 4.0, Unix	WebSphere Commerce Suite Service Provider 3.1.2, 3.2; WebSphere Application Server Enterprise Edition 4.0; WebSphere Application Server Advanced Edition 3.0.2.1; WebSphere Application Server 3.0.2.2-3.5.3	A vulnerability exists because predictable sequence numbers are used for session IDs when issuing cookies, which could let a malicious user gain unauthorized access.	Patch available at: http://www-4.ibm.com/software/webservers/appserv/efix_new.html	WebSpere Application Server Predictable Session ID	Medium	Bug discussed in newsgroups and websites.
Joerg Wendland[22]	Unix	pam-pgsql 0.9.2	A vulnerability exists in 'pam-psql' because SQL queries can be manipulated via any authentication medium, which could let a malicious user obtain access to restricted resources.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=24083	Pam-PSQL Remote SQL Query Manipulation	Medium	Bug discussed in newsgroups and websites.
Joerg Wendland[23]	Unix	libnss-pgsql 0.9.0	A vulnerability exists in the NSS (Name Service Switch) module, 'libnss-pgsql,' because SQL queries can be manipulated via a HTTP request, which could let a malicious user gain access to restricted resources.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=24083	LibNSS-PgSQL Remote SQL Query Manipulation	Medium	Bug discussed in newsgroups and websites.

[18] Caldera International, Inc. Security Advisory, CSSA-2001-033.0, September 7, 2001.
[19] Conectiva Linux Security Announcement, CLA-2001:425, September 11, 2001.
[20] Bugtraq, September 19, 2001.
[21] Bugtraq, September 19, 2001.
[22] RUS-CERT Advisory 2001-09:01, September 10, 2001.
[23] RUS-CERT Advisory 2001-09:01, September 10, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
John E. Davis[24]	Unix	MOST 4.4-4.9.1	A buffer overflow vulnerability exists due to improper bounds checking, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://security.debian.org/dists/stable/updates/main/	MOST Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Khamil Landross and Zack Jones[25]	Windows 95/98/ME/ NT 4.0/2000	EFTP 2.0.7.337	Multiple vulnerabilities exist: a vulnerability exists when a 'size' or 'mdtm' command is submitted, which could let a malicious user obtain sensitive information; usernames and passwords are stored in the file \Program Files\eftp2\eftp 2users.dat in clear text; and a buffer overflow vulnerability exists when a '*.lnk' file that contains a certain value is uploaded, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	EFTP Multiple Vulnerabilities	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit script has been published for the directory structure information disclosure vulnerability and the buffer overflow vulnerability. There is no exploit code required for the password vulnerability.
Leon J. Breedt[26]	Unix	pam-pgsql 0.5.1	A vulnerability exists in the PAM authentication module, 'pam-psql,' which could let a malicious user gain access to restricted resources.	No workaround or patch available at time of publishing.	Pam-PSQL Remote SQL Query Manipulation	Medium	Bug discussed in newsgroups and websites.
Merit[27]	Unix	RLMadmin 3.8M, 5.01	A symbolic link vulnerability exists in the 'rlmadmin' management utility, which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	RADIUS Server RLMadmin Symbolic Link	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Michael Boehme[28]	Multiple	Web Discount E-Shop Online-Shop System 1.0	A vulnerability exists in the default implementation due to insufficient sanitization from untrusted sources, which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	WebDiscount E-Shop Remote Arbitrary Command Execution	Medium	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
Microsoft[29]	Windows 95/98/ME/ NT 4.0/2000	Outlook Express 6.0	A vulnerability exists which allows an e-mail message of content-type 'text/plain' to execute specifically crafted scripting components. *Note: Scripting is not allowed by default. This security feature must be turned off in order to exploit this vulnerability.*	No workaround or patch available at time of publishing.	Outlook Express 6 Plain Text Message Script Execution	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[24] Debian Security Advisory, DSA 076-1, September 18, 2001.
[25] Bugtraq, September 12, 2001.
[26] RUS-CERT Advisory 2001-09:01, September 10, 2001.
[27] Securiteam List Digest, September 12, 2001
[28] SecurityFocus, September 15, 2001.
[29] Bugtraq, September 12, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[30]	Windows NT 4.0	Index Server 2.0	A vulnerability exists in the 'sqlqhit.asp' sample file, which is installed by default. This could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Index Server 2.0 File Information and Path Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[31]	Windows NT 4.0	Windows NT Terminal Server, NT 4.0, NT 4.0SP1-SP6a	A Denial of Service vulnerability exists when the RPC (Remote Procedure Call) Endpoint Mapper is sent a particular type of malformed data.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-048.asp	Windows NT RPC Endpoint Mapper Denial of Service	Low	Bug discussed in newsgroups and websites.
Multiple Vendors[32]	Multiple	RSA Security BSAFE SSL-J SDK 3.0-3.1; Cisco iCDN 2.0	A vulnerability exists in the SSL session caching feature, which could let a malicious user bypass the client authentication and use a bogus client certificate.	**RSA Security:** http://www.rsasecurity.com/support/bsafe/index.html **Cisco:** http://www.cisco.com.	RSA BSAFE SSL-J Authentication Bypass	Medium	Bug discussed in newsgroups and websites.
Oracle Corporation[33]	Multiple	Oracle 9i Application Server	A vulnerability exists when the server is sent an HTTP request for a non-existent .jsp file, which could let a malicious user obtain sensitive information.	Patch available at: http://otn.oracle.com/software/tech/java/servlets/content.html	Oracle Application Server Path Revealing	Medium	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
Pi-Soft[34]	Windows 95/98/ME/ NT 4.0/2000	SpoonFTP 1.1	A directory traversal vulnerability exists when a 'cd' command is submitted, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.pi-soft.com/spoonftp/sftp.exe	Pi-Soft SpoonFTP Directory Traversal	Medium	Bug discussed in newsgroups and websites.
ProFTPD Project[35]	Unix	ProFTPD 1.2pre9 & prior	A vulnerability exists because reverse-resolved hostnames are not forwarded to verify that the IP address matches of the client matches DNS records, which could let a remote malicious user bypass access control lists or have false information logged.	No workaround or patch available at time of publishing.	ProFTPD Client Hostname Resolving	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Randy Parker[36]	Unix	Power Up HTML 0.8033beta	A directory traversal vulnerability exists because metacharacters from HTTP requests are not filtered, which could let a malicious user view sensitive information or execute arbitrary code.	No workaround or patch available at time of publishing.	Power Up HTML Directory Traversal Arbitrary File Disclosure	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[30] Oxygen3 24h-365d, September 17, 2001.
[31] Microsoft Security Bulletin, MS01-048, September 10, 2001.
[32] Cisco Security Advisory, CI-01.12, September 12, 2001.
[33] Bugtraq, September 17, 2001.
[34] Bugtraq, September 20, 2001.
[35] Bugtraq, September 7, 2001.
[36] Securiteam, September 9, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
RedHat[37]	Unix	Linux 7.0	A vulnerability exists in versions of Apache webserver that are shipped with Red Hat Linux 7.0, which could allow a remote malicious user to obtain sensitive information.	No workaround or patch available at time of publishing.	Linux Apache Remote Username Enumeration	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
SeaGlass Technol-ogies, Inc.[38]	Unix	sglMerchant 1.0	A directory traversal vulnerability exists because user-supplied input is not properly filtered, which could let a remote malicious user gain sensitive information.	No workaround or patch available at time of publishing.	sglMerchant Directory Traversal	Medium	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
Source Force[39]	Multiple	Vibechild Directory Manager 0.9	An input validation vulnerability exists due to a script in the PHP's 'passthru()' function, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Vibechild Directory Manager Command Execution	**High**	Bug discussed in newsgroups and websites.
Speech10[40]	Unix	SpeechD 0.1, 0.2	A vulnerability exists which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	SpeechD Privileged Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Symantec[41]	Windows 20000	Norton AntiVirus for MS Exchange 2.5	A vulnerability exists in Microsoft Exchange 2000 when running with Norton AntiVirus for Microsoft Exchange, which could disclose mail directory paths to a malicious user.	Temporary Workaround (Bugtraq): Customize Norton AntiVirus for Microsoft Exchange 2000's notification feature (using 'Global Options') that sends rejected messages back to the sender to not include the mailbox location in the bounced message.	Norton AntiVirus for Microsoft Exchange 2000 Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Textor Web-masters Ltd.[42]	Multiple	ListRec.pl 1.0	A vulnerability exists because 'listrec.pl' does not adequately validate user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	ListRec.pl Input Validation	**High**	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
Trend Micro, Incor-porated[43]	Windows NT 3.5/4.0	InterScan eManager 3.51, 3.51j; InterScan VirusWall for Windows NT 3.5, 3.51	A buffer overflow vulnerability exists in some CGI programs that are used by the management console, which could let a malicious user execute arbitrary code.	Patch available at: http://www.trendmicro.co.jp/esolution/solutionDetail.asp?solutionID=3142	InterScan eManager Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[37] Bugtraq, September 12, 2001.
[38] Securiteam, September 9, 2001.
[39] Bugtraq, September 4, 2001.
[40] Bugtraq, September 11, 2001.
[41] Bugtraq, September 7, 2001.
[42] Bugtraq, September 12, 2001.
[43] SNS Advisory No. 42, September 12, 2 001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Xcache Technol-ogies[44]	Windows NT 4.0/2000	Xcache 2.0, 2.1	A vulnerability exists when a request is made for a page or a page within a folder that is not cached, which could let a malicious user obtain sensitive information.	Users of Xcache can obtain the patch by contacting: support@xcache.com	Xcache Path Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
ZyXEL[45]	Multiple	Prestige 642R	A vulnerability exists in the WAN interface because internal IP addresses are not filtered, which could let a malicious user gain unauthorized access to the administration interface.	No workaround or patch available at time of publishing.	Prestige 642R Router WAN Port Filter Bypass	Medium	Bug discussed in newsgroups and websites.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between September 5 and September 21, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 19 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
September 21, 2001	Mimedefang-1.4.tar.gz	A flexible MIME e-mail scanner designed to protect Windows clients from viruses and other harmful executables which works with Sendmail 8.10 / 8.11 and will alter or delete various parts of a MIME message according to a flexible configuration file.

[44] IRM Security Advisory No. 001, September 21, 2001.
[45] Bugtraq, September 18, 2001.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
September 20, 2001	Gps-0.8.0.tar.gz	Ghost Port Scan is an advanced port scanner and a firewall rule disclosure tool that uses IP & ARP spoofing, sniffing, stealth scanning, ARP poisoning, IP fragmentation, and other techniques to perform stealth and untraceable information collection.
September 19, 2001	Netl-1.09.tar.gz	A network logger/sniffer suitable for TCP/IP over Ethernet and loopback that is capable of logging everything from pings to Telnet, including low level IP like SYNs and RSTs.
September 17, 2001	Cyellow-0.01.tar.gz	An example code for Fun and Games with FreeBSD Kernel modules that contains examples for all the different kernel alteration methods plus several small tools that can also be used for detection and defense.
September 17, 2001	Ettercap-0.6.0.tar.gz	A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
September 17, 2001	Fbsdfun.htm	"Fun and Games with FreeBSD Kernel Modules" describes techniques for kernel hacking using kernel modules and kmem patching. Also contains information on how to intercept system calls and other calls in the kernel by altering the corresponding call table, shows how to alter these tables by writing to kernel memory and gives an example of patching the kernel directly without the use of modules and an example is given on how the symbol table in the kernel can be altered.
September 12, 2001	**Eftpsizemap.pl**	**Perl script which exploits the EFTP Directory Structure Information Disclosure vulnerability.**
September 12, 2001	**Ex_eftpd.c**	**Script which exploits the EFTP Buffer Overflow Vulnerability.**
September 11, 2001	Dosadsl812.java	Denial of service attack against a 3com ADSL 812 router in Java, which resets the router without any password.
September 11, 2001	Dscan-0.5.tar.gz	A distributed port scanner that scans from many hosts.
September 11, 2001	Irs14.exe	IP Restrictions Scanner (IRS) is a Windows NT/2k tool, which finds out which network restrictions have been set for a particular service on a host. It also combines "ARP Poisoning" and "Half-Scan" techniques and tries totally spoofed TCP connections to the selected port of the target.
September 11, 2001	Km.pl	Remote Denial of Service exploit for the Kazaa and Morpheus vulnerability.
September 10, 2001	Cso.c	A remote exploit for the CGIemail vulnerability.
September 10, 2001	**Msgchkx.c**	**Exploit script for the Digital Unix MSGCHK MH_PROFILE Symbolic Link and MSGCHK Buffer Overflow vulnerability.**
September 10, 2001	**Msgchkx.sh**	**Exploit script for the Digital Unix MSGCHK MH_PROFILE Symbolic Link and MSGCHK Buffer Overflow vulnerability.**
September 7, 2001	Altering_arp_tables_v_1.00.htm	This paper is dedicated to ARP tables and how to alter them remotely. Also includes a couple of implementations of ARP poisoning in a bridge-based segment.
September 7, 2001	Gps-0.7.0.tar.gz	Ghost Port Scan is an advanced port scanner and a firewall rule disclosure tool. Uses IP & ARP spoofing, sniffing, stealth scanning, ARP poisoning, and other techniques to perform stealth and untraceable information collection.
September 6, 2001	Jolt2.c	Script which exploits the DLink IP Fragment Denial Of Service vulnerability.
September 5, 2001	Smsspoof-1.1.tar.gz	An application that allows you to send spoofed SMS messages with a palm pilot.

Trends

Probes/Scans:

- **There has been an increase in scans of port 23 probing for the Multiple Vendor TelnetD vulnerability. (For more information, see the Multiple Vendor TelnetD Buffer Overflow vulnerability described in CyberNotes 2001-15 [July 30, 2001] located at http://www.nipc.gov/cybernotes/2001/cyberissue2001-15.pdf.)**
- **CERT/CC continues to observe increased network reconnaissance activity and a significant increase in the number of generalized port scans of hosts.**

Other:

- **The National Infrastructure Protection Center expects to see an upswing in incidents as a result of the tragic events of September 11, 2001. For more information, see NIPC ADVISORY 01-020, available at http://www.nipc.gov/warnings/advisories/2001/01-020.htm.**
- **The National Infrastructure Protection Center has received numerous reports that a new worm, named W32.Nimda.A@MM (see Virus Section), is propagating extensively through the Internet worldwide. The worm is exhibiting many traits of recently successful malicious code attacks such as CODE RED but it is not simply another version of that worm. For more information, see NIPC ADVISORY 01-022, available at: http://www.nipc.gov/warnings/advisories/2001/01-022.htm.**
- **The National Infrastructure Protection Center expects an increase in Distributed Denial of Service (DDoS) attacks. For more information, see NIPC ADVISORY 01-021 located at: http://www.nipc.gov/warnings/advisories/2001/01-021.htm.**
- **Recently, the cyber security community received numerous reports of intruders using the buffer overflow vulnerability in the Telnet daemon program. For more information, see NIPC ASSESSMENT 01-019, available at: http://www.nipc.gov/warnings/assessments/2001/01-019.htm. This vulnerability has the potential to impact the victim by allowing an intruder to copy, delete, or execute any program on the victim's system. A new worm called "x.c," designed to exploit this vulnerability, has also been discovered.**
- **The CERT/CC has observed a significant increase in activity resulting in compromises of home user machines. Many home users do not keep their machines up to date with security patches and workarounds, do not run current anti-virus software, and do not exercise caution when handling e-mail attachments. Intruders know this, and we have seen a marked increase in intruders specifically targeting home users who have cable modem and DSL connections.**
- **A modified variant of the Code Red worm, called Code Blue, has emerged. This worm launches attacks against an IP address (211.99.196.135) associated with the Web site of a Chinese network security provider.**

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *Note: At times, viruses may contain names or content that may be considered offensive.*

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Nimda	File, Worm	New to Table	September 2001
2	W32/SirCam	Worm	Stable	July 2001
3	W32/Magistr	File, Worm	Slight Decrease	March 2001
4	W32/Funlove	File	Slight Increase	November 1999
5	VBS/Haptime	Script	New to Table	May 2001
6	W32/Hybris	Worm	Slight Decrease	November 2000
7	VBS/Kakworm	Script	Slight Decrease	December 1999
8	W32/Apost	File, Worm	New to Table	September 2001
9	VBS/Loveletter	Script	Decrease	March 2000
10	W95/CIH	File	Return to Table	July 1998

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **208** distinct viruses are currently considered "in the wild" by anti-virus experts. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines.

Dilo.667 (DOS Virus): This is a DOS virus that infects .com files. The infected files are usually corrupted and cannot be repaired.

OF97/Jerk-J (Office 97 Macro Virus): This is a variant of the OF97/Jerk Microsoft Office macro virus. The virus attempts to infect Word documents and Excel spreadsheets, but because part of the Excel macro code is removed, affected spreadsheets will not be able to transmit the virus.

PE_MTX_II.A (Aliases: MTX_II.A, TROJ_MTX_II.DLL, PALM_MTX_II.A) (File Infector Worm): This polymorphic Windows file infector is a component of the MTX_II.A virus that infects files, propagates copies of itself via e-mail, and drops a Palm application. Upon execution, it prompts the user of the target system to choose whether it should infect a certain file so that it may continually infect files. The mother virus, which is unencrypted, copies itself in the Windows System directory to a random filename with a .DLL extension. Its infected file extracts the virus portion to the Windows System directory into a random filename with the extension .TMP. It then creates a separate process and lets the original file execute. Next it informs the user that it has created the copy of the virus file with a random filename. It displays the following message: "THIS IS THE CURRENT VIRUS FILE NAME: C:\WINDOWS\SYSTEM\<random filename>.DLL." It then searches the Hard Drive for a WS2_32.DLL file and a WSOCK32.DLL file and prompts the user to choose whether to infect the files by displaying the following message:

CAN I TRY TO INFECT THIS FILE?
C:\WINDOWS\SYSTEM\WS2_32.DLL
<OK button> <Cancel button>

If the user clicks the OK button, it then infects the identified file. Otherwise it ignores it. The virus also creates a backup of the file to a file with the extension ".---." It patches the exported functions, "recv," "send," and "connect" which point to the virus code. After it infects the files, it displays the following message identifying the back up it created of the infected file:

THIS FILE WAS INFECTED:
C:\WINDOWS\SYSTEM\WS2_32.---

It then loads the IMAGEHLP.DLL library and uses the SearchTreeForFile API to search for the following files:

NAPSTER.EXE
WINZIP32.EXE
EUDORA.EXE
WINRAR.EXE

W32DSM89.EXE
WZSEPE32.EXE
WSCRIPT.EXE
ICQ.EXE

The virus searches for the above files to infect, but anyone can modify these files to infect other files as well. The virus does not infect files that are less than 8,192 Bytes (2000h) or greater than 9,437,184 Bytes (900000h) in file size. It also does not infect files that contain any of the following 2-byte sequences in the filename: "AV," "00," "VS," "RW," "VC," or "GP." Before it infects a file, it checks the first byte on the entry point address of the PE file. It does not infect the file if the first byte is a PUSHF instruction (9Ch) or a PUSHA instruction (60h). This ensures that it does not reinfect previously infected files.

PE_NIMDA.A (Aliases: NIMDA.A, W32/Nimda.A@mm, CV-5, Minda, Concept Virus, Code Rainbow) (File Infector Worm): This virus has been reported extensively in the wild. It uses three modes for propagation. It spreads via e-mail, network shares, or through servers with IIS installed using the IIS Web Directory Traversal exploit. The PE worm arrives as an embedded README.EXE file or as attachment in an e-mail that has an empty message body and a usually empty subject field. It does not require that the target user double-clicks the attachment for it to execute. This worm uses the vulnerability that is known as Automatic Execution of Embedded MIME type. More information about this vulnerability is explained at Microsoft's Security Bulletin (MS01-020), located at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-020.asp. The embedded EXE file, cannot be seen/viewed in MS Outlook. Upon execution this worm drops the file mepXXXX.tmp.exe in the C:\Windows\Temp directory, which is an eml format mail (a content-type of audio/x-wav with an executable attachment type). The executable temp file contains the file attachment that this worm sends to its addressed e-mails. The Wininit.ini has an entry that sets one of the mepXXXXX.tmp.exe files to a null value, deleting one of the mepXXXXX.tmp.exe files. The typical name of the file attachment is readme.exe but there have been reports of file attachments with the extensions .WAV and .COM. Wininit.ini contains an entry that sets one of the mepXXXX.tmp.exe files to a null value, deleting one of the mepXXXXX.tmp.exe files. Along with the MEPxxxxx.TMP.EXE file dropped in Windows temp folder, it also drops a copy of itself as LOAD.EXE and overwrites the RICHED20.DLL in the Windows System folder. It sets the attributes of both files as "Hidden" and "System." To execute upon system startup, it creates an entry in the shell key of the boot section of SYSTEM.INI so that the line contains the following:

Shell="Explorer.exe load.exe –dontrunold."

The worm drops another copy of itself as MMC.EXE in the Windows folder and propagates via e-mail using its own SMTP engine and also through Messaging APIs. It may execute when the recipient of its carrier e-mail opens the e-mail using Microsoft Outlook or Outlook Express. It makes use of an exploit on these e-mail clients when the receiving user displays the sent e-mail in HTML format that contains frames. The worm also propagates through shared drives. Similar to PE_FUNLOVE.4099, the worm searches the infected machine's network for shared folders with write access. If it finds one, it drops a randomly named .NWS (Newsgroup posting) or .EML file. These dropped files also contain the worm as an attachment. The .EML dropped file has a DLL file structure. This worm also drops a copy of itself as the RICHED20.DLL file in shared folders that have the extensions, .EXE, .EML, or .DOC. This worm contains codes that enable it to infect certain HTML, HTM, or ASP files. The default files that it modifies are as follows:

README.HTM
README.HTML
README.ASP
MAIN.HTM
MAIN.HTML
MAIN.ASP
INDEX.HTM
INDEX.HTML
INDEX.ASP
DEFAULT.HTM
DEFAULT.HTML
DEFAULT.ASP

In certain circumstances, the worm "infects" HTML, HTM, or ASP files other than those mentioned above. Default files or not, the infection routine of this worm is the same: it adds a JavaScript command that opens the README.EML file when the infected file is executed. The worm occasionally infects executables files. The worm infection is pre-pending, which means that it attaches a copy of its binary code at the start of the original host. Similar to TROJ_BLUECODE.A, this worm spreads to machines with IIS installed using the IIS Web Directory Traversal exploit, in which a request is sent to the target machine, forcing it to download a copy of ADMIN.DLL from the infected machine through TFTP (trivial file transfer protocol). The worm then executes the last phase of its exploit by forcing the remote computer to copy the recently downloaded .DLL file into its root directory as C:\ADMIN.DLL, D:\ADMIN.DLL, and E:\ADMIN.DLL. This worm contains a user-defined resource within its code. For every copy it makes, either in the local file system, in the network shares, or in the infected files, the worm modifies 4 bytes of this resource. Also, the file executes a script that adds the guest user into the local Guest group account and the local Administrators group account. This action allows Administrative privileges to the guest user. Afterwards, it ensures the shared drive c$=C:\. When the worm is run, it spawns multiple copies of itself by dropping several executable files and running them. Occasionally, to hide these spawned copies from the user, they register themselves as services under Win 9x. It also enables sharing of all the drives that it shows in the modifications it does in the registry. The modification follows the below format:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\
<drive>$
<drive> equals the letter of the drive it shares from C to Z.

The worm file contains the following text:

"-Concept Virus (CV) V.5, Copyright (C) 2001 R.P.China"

Umisy.2322 (DOS Virus): This is a DOS virus that overwrites .com files. When it is executed, it displays the following message:

UMISYS RamDoubler v. 2.7
Copyright UMISYS 1989-1996. All rights reserved.

VBS/BlueMail.A@mm (Visual Basic Script Worm): The worm arrives as embedded VBScript code and makes use of the scriptlet.typelib/Eyedog vulnerability. It is received in an e-mail containing the following information:

From: Microsoft-FunnyMail etc..
Subject: FW: Remember Windows 3.1?

Simply reading the e-mail message or viewing it in a preview pane (on an unpatched system - IE5.5 and higher includes this patch) is enough to infect your machine. Once activated, the worm copies itself to the file RUNDLL32.HTA in WINDOWS SYSTEM directory and then executes the file. It alters the registered owner of Windows by setting a registry key value:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\RegisteredOwner=H0axley

The worm creates a registry key to log its mailing action. This ensures that the mailing routine only takes place once:

HKEY_LOCAL_MACHINE\Software\Outlook.DeepBlue=Outlook.DeepBlue by H0axley

If this value is not present, the worm mails itself to all recipients found in the Microsoft Outlook Address book. It then searches for INETPUB\WWWROOT\INDEX.HTML, copies itself to the file INETPUB\WWWROOT\SAVE0001.HTML for backup. It creates an infected INETPUB\WWWROOT\IMPORTANT.HTML and creates INETPUB\WWWROOT\README.txt with string "Outlook.DeepBlue Version 1.0 by H0axley." Next, it creates a new INETPUB\WWWROOT\INDEX.HTML containing the text:

Temporarily Closed
<!-- This server is infected by 'Outlook.DeepBlue' virus by H0axley (Thanks to Zulu) -->
We are sorry but this page is temporarily closed. We are testing the new DeepBlue©
system. Would you like to read some very funny jokes ?
(NOTE: This link doesn't work if you don't enable Microsoft© ActiveX© multimedia
when asked to do so ;-)

The worm also creates a blue message box entitled, "Microsoft Funnymail (Powered by Outlook.DeepBlue by H0axley)" which reads:

Windows
A fatal exception 0E has occured at F0AD:42494C4C
Press any key to continue.

W32/Creepy.a@MM (Aliases: Creepy, W32/Creepy@MM, Win32.Creep.A@mm) (Win32 Virus): This mass-mailing worm sends itself to all entries found in the Microsoft Outlook Address Book and alters the default start page and search page used by Microsoft Internet Explorer. When run, a DOS window is displayed. Immediately after displaying this window an Outlook prompt appears. Clicking CANCEL will remove the Outlook prompt as well as the DOS window message. The worm then sends an e-mail message with the following information.

To:
BCC: All recipients in the MS Outlook address book
Subject: Leuk programmaatje!
Attachment: (Last 8 characters in the name of the executable).exe often Hypnose.exe

Running the attachment infects the local system. The worm creates two registry run keys to load itself at startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MyApp=%WormPath% (varies)
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\MyApp=%WormPath% (varies)

An additional registry key value is created:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\SafeSites\ie.search.msn.com= http://www.serverbeat.nl/redir.php?http://www.protagonist.nl/redir.php?http://www.uniserver.nl/redir.php

The default start page of Internet Explorer is set to http://www.de-isp.nl.

W32.Kan (Alias: Win32.Kanban) (Win32 Virus): This is a very simple virus. The viral body is only 132 bytes in size. When executed, it obtains the path to the \Windows folder, and then sets the \Windows folder as the current folder. Next, the virus goes into a simple FindFirst/FindNext loop, looking for executable files. It attempts to infect all executable files that it finds. The only way that the virus can exit the loop is when an error occurs or when it is unable to find any additional executable files. The viral body of this virus is only 132 bytes in size. The reason is that this virus uses the Invictus.dll files in its infection routine. The virus simply passes the name of the file that should be infected to a function in Invictus.dll named "_infect_file." It is this function that actually infects the file.

W97M.Sting: (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents and overwrites the global template, Normal.dot. The virus changes the printer and document settings 30 days after infection. It also modifies the Autoexec.bat so that the file is run when you start Windows.

WM97/Hope-AG (Word 97 Macro Virus): This is a member of the WM97/Hope virus family, which deletes the Tools/Macro and Tools/Options menu choices from the toolbar in an attempt to hide itself.

WM97/Metys-L (Word 97 Macro Virus): This is a member of the WM97/Metys family. On 18 December the virus displays a message box saying "Happy Birthday Jess! To celebrate, we're going to see how lucky you are," followed by the user's username and "Click the OK button below to roll a number. If your number matches that of the dealer, you win!." There is then a random chance that the virus will password protect the user's document with a random numeric password.

Trojans

Trojan Horse programs have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
Adshow	N/A	CyberNotes-2001-17
AOL.PWSteal.86016	N/A	CyberNotes-2001-14
Artic	0.6 beta	CyberNotes-2001-14
Asylum	N/A	CyberNotes-2001-18
Backdoor.Bionet.318	N/A	CyberNotes-2001-13
Backdoor.Bionet.40a	N/A	CyberNotes-2001-14
Backdoor.Darkirc	N/A	CyberNotes-2001-15
Backdoor.G_Door	N/A	CyberNotes-2001-18
Backdoor.IRC.Critical	**N/A**	**Current Issue**
Backdoor.IRC.Flood	N/A	CyberNotes-2001-16
Backdoor.MiniCommander:	N/A	CyberNotes-2001-16
Backdoor.Penrox	N/A	CyberNotes-2001-17
Backdoor.SMBRelay	N/A	CyberNotes-2001-10
Backdoor.Teste	N/A	CyberNotes-2001-16
Backdoor.Way	N/A	CyberNotes-2001-18
Backdoor.WLF	N/A	CyberNotes-2001-08
Backdoor-QN	N/A	CyberNotes-2001-13
Backdoor-QO	N/A	CyberNotes-2001-13
Backdoor-QR	N/A	CyberNotes-2001-13
Backdoor-QT	N/A	CyberNotes-2001-14
Backdoor-QV	N/A	CyberNotes-2001-14
Backdoor-QZ	N/A	CyberNotes-2001-14
BAT.Black	N/A	CyberNotes-2001-11
Bat.FAGE.1482	N/A	CyberNotes-2001-15
Bat.Hexvirus.1414	N/A	CyberNotes-2001-15
Bat.PG94.3964	N/A	CyberNotes-2001-15
BAT.Trojan.DeltreeY	N/A	CyberNotes-2001-07
BAT.Trojan.Tally	N/A	CyberNotes-2001-07
BAT_FORMATC.K	N/A	CyberNotes-2001-13
BioNet	3.13	CyberNotes-2001-07
BSE Trojan	N/A	CyberNotes-2001-07
CodeRed II	II	CyberNotes-2001-16
DMsetup.IRC.Worm	N/A	CyberNotes-2001-13
DonaldD.Trojan.C	**N/A**	**Current Issue**
EIC.Trojan	N/A	CyberNotes-2001-14
Eurosol	N/A	CyberNotes-2001-10
Fatal Connections	2.0	CyberNotes-2001-09
Freddy	beta 3	CyberNotes-2001-09
Gift	1.6.13	CyberNotes-2001-09
Goga	N/A	CyberNotes-2001-12
Gribble	**N/A**	**Current Issue**
HackTack	N/A	CyberNotes-2001-18
IRC/FinalBot	N/A	CyberNotes-2001-18
Jammer Killah	1.2	CyberNotes-2001-10

Trojan	Version	CyberNotes Issue #
JAVA_STORM.A	N/A	CyberNotes-2001-13
JS.Alert.Trojan	**N/A**	**Current Issue**
JS.Seeker.B	N/A	CyberNotes-2001-18
JS.StartPage	N/A	CyberNotes-2001-07
JS_OFFENSIVE.A	N/A	CyberNotes-2001-17
JS_ZOPA.A	N/A	CyberNotes-2001-14
KillMBR.g	N/A	CyberNotes-2001-16
Lil Witch FTP	**1.0**	**Current Issue**
Noob	4.0	CyberNotes-2001-09
PERL/WSFT-Exploit	N/A	CyberNotes-2001-11
Phoenix	2.1.28	CyberNotes-2001-18
PWS.Cain.dr	**N/A**	**Current Issue**
PWSteal.Trojan.D	N/A	CyberNotes-2001-13
QDel172	N/A	CyberNotes-2001-17
Remote Shell Trojan	**N/A**	**Current Issue**
SadCase.Trojan	N/A	CyberNotes-2001-09
Scarab	1.2c	CyberNotes-2001-10
SennaSpy Generator	N/A	CyberNotes-2001-13
StealVXS	N/A	CyberNotes-2001-17
Troj/Futs	N/A	CyberNotes-2001-07
Troj/Keylog-C	N/A	CyberNotes-2001-08
Troj/PsychwardB	N/A	CyberNotes-2001-14
Troj/Slack	N/A	CyberNotes-2001-14
Troj/Unite-C	N/A	CyberNotes-2001-09
TROJ_ALLGRO.A	N/A	CyberNotes-2001-17
TROJ_APOST.A	N/A	CyberNotes-2001-18
TROJ_ASIT	N/A	CyberNotes-2001-07
TROJ_BADTRANS.A	N/A	CyberNotes-2001-08
TROJ_BADY	N/A	CyberNotes-2001-15
TROJ_BCKDOR.G2.A	N/A	CyberNotes-2001-11
TROJ_CAFEIN111.A	N/A	CyberNotes-2001-14
TROJ_CHOKE.A	N/A	CyberNotes-2001-13
TROJ_DSNX.A	N/A	CyberNotes-2001-17
TROJ_EUTH.152	N/A	CyberNotes-2001-08
TROJ_FUNNYFILE.A	N/A	CyberNotes-2001-09
TROJ_HAI.A	N/A	CyberNotes-2001-17
TROJ_HAVOCORE.A	N/A	CyberNotes-2001-09
TROJ_ICMPBOMB.A	N/A	CyberNotes-2001-17
TROJ_IDENTD.B	N/A	CyberNotes-2001-11
TROJ_IE_XPLOIT.A	N/A	CyberNotes-2001-08
TROJ_INCOMM16A.S	N/A	CyberNotes-2001-09
TROJ_INVALID.A	N/A	CyberNotes-2001-18
TROJ_IRC_NETOL.A	N/A	CyberNotes-2001-14
TROJ_JOINER.I	N/A	CyberNotes-2001-08
TROJ_KEYLOG.25	N/A	CyberNotes-2001-17
TROJ_LASTWORD.A	N/A	CyberNotes-2001-09
TROJ_LATINUS.SVR	N/A	CyberNotes-2001-12
TROJ_LEAVE.A	N/A	CyberNotes-2001-13
TROJ_LINONG.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.B	N/A	CyberNotes-2001-13
TROJ_MATCHER.A	N/A	CyberNotes-2001-08
TROJ_MEGA.A	N/A	CyberNotes-2001-12
TROJ_MODNAR.A	N/A	CyberNotes-2001-17
TROJ_MOONPIE.A	N/A	CyberNotes-2001-11
TROJ_MSWORLD.A	N/A	CyberNotes-2001-12
TROJ_MTX.A.DLL	N/A	CyberNotes-2001-09

Trojan	Version	CyberNotes Issue #
TROJ_MUSTARD.A	**N/A**	**Current Issue**
TROJ_NARCISSUS.A	N/A	CyberNotes-2001-09
TROJ_NEWPIC.A	N/A	CyberNotes-2001-17
TROJ_NEWSAGENT.A	N/A	CyberNotes-2001-16
TROJ_NEWSFLOOD.A	N/A	CyberNotes-2001-13
TROJ_OPTIX.SVR	N/A	CyberNotes-2001-17
TROJ_PICSHOW.A	N/A	CyberNotes-2001-10
TROJ_PSW.GINA.A	N/A	CyberNotes-2001-13
TROJ_SCOUT.A	N/A	CyberNotes-2001-08
TROJ_SIRCAM.A	N/A	CyberNotes-2001-15
TROJ_SPYBOY.A	N/A	CyberNotes-2001-18
TROJ_VAMP.A	N/A	CyberNotes-2001-13
TROJ_VBSWG_2B	N/A	CyberNotes-2001-07
TROJ_VOTE.A		**Current Issue**
TROJ_WARHOME.A	N/A	CyberNotes-2001-12
TROJ_WHISTLER.A	**N/A**	**Current Issue**
TROJ_WINMITE.10	N/A	CyberNotes-2001-08
TROJ_ZERAF.A	N/A	CyberNotes-2001-18
Trojan.Assault.10	10	CyberNotes-2001-15
Trojan.Bat.Live4:	N/A	CyberNotes-2001-16
Trojan.Billrus.Texto	N/A	CyberNotes-2001-14
Trojan.Diagcfg	N/A	CyberNotes-2001-15
Trojan.JS.Clid.gen	N/A	CyberNotes-2001-17
Trojan.JS.Cover	N/A	CyberNotes-2001-18
Trojan.Lornuke	N/A	CyberNotes-2001-14
Trojan.Offensive	N/A	CyberNotes-2001-17
Trojan.Pounds	N/A	CyberNotes-2001-18
Trojan.PSW.M2.14	N/A	CyberNotes-2001-07
Trojan.Taliban	N/A	CyberNotes-2001-07
Trojan.VBS.PWStroy	N/A	CyberNotes-2001-14
Trojan.VirtualRoot	N/A	CyberNotes-2001-16
Trojan.W32.FireKill	N/A	CyberNotes-2001-07
Trojan.Xtratank	N/A	CyberNotes-2001-17
Trojan.Zeraf	N/A	CyberNotes-2001-17
Trojan.ZeroBoot	**N/A**	**Current Issue**
Trojan/PokeVB5	N/A	CyberNotes-2001-07
VBS.AutoExec.Trojan	N/A	CyberNotes-2001-16
VBS.Blank.A	N/A	CyberNotes-2001-14
VBS.Fiber.C	N/A	CyberNotes-2001-18
VBS.Lumorg	N/A	CyberNotes-2001-09
VBS.Natas	N/A	CyberNotes-2001-16
VBS.Over.Trojan	N/A	CyberNotes-2001-10
VBS.Phybre	N/A	CyberNotes-2001-12
VBS.Reset	N/A	CyberNotes-2001-12
VBS.SystemColor.A	N/A	CyberNotes-2001-11
VBS.Trojan.Icon	N/A	CyberNotes-2001-18
VBS.Trojan.Lariara	N/A	CyberNotes-2001-18
VBS.Zeichen.A	N/A	CyberNotes-2001-08
VBS.Zync.A	N/A	CyberNotes-2001-17
VBS_HAPTIME.A	N/A	CyberNotes-2001-09
VBS_IESTART.A	N/A	CyberNotes-2001-11
W32.BrainProtect	N/A	CyberNotes-2001-07
W32.Leave.B.Worm	N/A	CyberNotes-2001-14
Y3K Rat	1.6	CyberNotes-2001-11

Backdoor.IRC.Critical: This is a backdoor Trojan that allows unauthorized access to a compromised system. It allows a malicious user to control your computer using Internet Relay Chat (IRC). Normally, this backdoor Trojan horse is distributed as one large installation executable. Once run, this executable pretends to install a benign antivirus program, while in the background it installs the backdoor files in various places on the system. All the files in the C:\Program Files\Accessories\Backup\System\Critical folder are created with "Hidden" attributes, in an attempt to escape being noticed. In order to gain control of the compromised system, this Trojan horse does the following:

- It modifies the run= line of the C:\Windows\Win.ini file so that it becomes: run=C:\Windows\DskLoad.exe
- It makes the following modifications to the registry:
  - In the key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\mIRC it adds or modifies the value "DisplayName mIRC"
  - In the key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\mIRC it adds or modifies the value "UninstallString C:\program files\accessories\backup\system\critical\expl32.exe" –"uninstall"
  - In the key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run it adds the value "StubPath C:\Windows\DskLoad.exe"
  - In the key HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\KeyName it adds or modifies the value "MSSysDisk C:\Windows\DskLoad.exe"
  - Finally, IRC file extensions are hooked in HKEY_LOCAL_MACHINE\Software\Classes that call "C:\program files\accessories\backup\system\critical\expl32.exe" when chat files are opened.

The inserted file C:\Windows\Sys.exe is waiting for the user or a program to call the "sys" command. In DOS-based operating systems, the file Sys.com is used to make a data medium DOS bootable. On Windows computers, this file would reside in C:\Windows\Command\sys.com. However, when running "sys" from the command prompt, the viral C:\Windows\Sys.exe is run instead of the proper C:\Windows\Command\sys.com. This viral sys.exe installs Backdoor.Subseven.22 on the system allowing for even more control over the compromised system.

DonaldD.Trojan.C (Alias: Backdoor-AQ): This Trojan allows a malicious user to have remote access to the computer. It modifies the registry so that it runs when you start Windows. If the Trojan is run, it creates the following files:

\Windows\System\Rgl5max.exe
\Windows\System\Pon2dil.vxd

These files are loaded as a service when you start Windows. This is accomplished by making the following changes to the registry:

- The Trojan creates the key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\PON2DIL with the values:
  "StaticVxD pon2dil.vxd Start 00"
  and the key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\PEN2D with the value:
  "dxt <long string of byte sequences>"
  It also adds the value:
  "@ <long string of random characters>"
  to the keys:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Keyboard Layouts\0000080A
  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Time Zones\W. Europe

Gribble (Alias: Trojan.IRC.Gribble): This Trojan has been available an a web page that uses a Java Virtual Machine vulnerability in Internet Explorer to drop and execute the worm. More information about this Microsoft vulnerability can be found at: http://www.microsoft.com/technet/security/bulletin/MS00-075.asp. When the Trojan is executed, it creates "jb.vbs" file into the root of the current drive. Next the Trojan drops another VBS file, "C:\lipreffs.vbs." This file is executed when the system is restarted. It also starts to send large ICMP echo (ping) packets to the gnc.com. Next Gribble goes through all drives, and if it is able to locate a mIRC installation, it will create "script.ini" and modify the "mirc.ini" so, that it will be loaded when the IRC client is started. Finally the Trojan deletes "C:\jb.vbs." The modified "script.ini" will attempt a Denial of Service attack against grc.com when a connection is made with the mIRC client. The Trojan also sends offensive messages when another user joins a channel where the infected user is.

JS.Alert.Trojan: This is a JavaScript Trojan, which displays an alert window when the script is activated. The script was posted in several newsgroups. This script contains instructions to display a window alert as long as a boolean variable is "true." The condition is never modified and the boolean value will always remain true. Because of this, the window alert will be displayed constantly and it will never close. The only way to exit from this condition is to exit the program that is used to read the HTML message.

Lil Witch FTP (1.0): This is a simple ftp server, possibly to be used in conjunction with the Littlewitch remote access Trojan that originates from central America.

PWS.Cain.dr: This is a Trojan installation package that, if executed, places a password stealer on your computer.

Remote Shell Trojan (RST): This Trojan attacks Linux ELF binaries. It has replicating abilities: when run it will infect all binaries in /bin and the current working directory. It spreads through e-mail as well as replicating itself across the infected system. The Trojan installs a backdoor which listens for incoming connections on UDP port 5503 or higher, and allows remote malicious users to connect to, and take control of, an infected system. The Trojan is most dangerous if it is executed by a privileged user as it inherits the credentials of that user, effectively allowing it to take full control. Once a system is infected, the Remote Shell Trojan calls home to a UK-based website.

TROJ_MUSTARD.A (Aliases: MUSTARD, MUSTARD.A, I-Worm.Petik.d, W95.Pet_Tick.gen): This Trojan drops two components that enable it to replicate via Internet Relay Chat (IRC) and through e-mail. Upon execution, this Trojan drops an AVUPDATE.EXE file in the Windows directory. A known antivirus product uses the filename and icon of this dropped file so that it appears to be a legal program. It modifies the following line of the WIN.INI file so that it executes upon Windows startup:

run=C:\Windows\System\AVUPDATE.EXE

This Trojan creates a SCRIPT.INI file with instructions that enable it to propagate copies of itself via IRC. It also creates a SEND.VBS file with instructions that enable it to propagate as an attachment in e-mails it sends.

TROJ_VOTE.A (Aliases: WTC, W32/Vote@mm, I-Worm.Vote): This Trojan is currently spreading in the wild. It is a destructive, mass-mailing Trojan that was created using Visual Basic 5. The Trojan propagates via Microsoft Outlook by sending e-mails to all addresses listed in an infected user's address book. It arrives in an e-mail with the following:

Subject: Fwd: Peace BeTween AmeriCa And IsLam!
Message Body: Hi!
iS iT A waR Against AmeriCa Or IsLam!
Let's Vote To Live in Peace!
Attachment: WTC.EXE

Upon execution, this worm opens the following sites:

http://us.f1.&ltblocked>.com/users/da36d538/bc/TimeUpdate.exe?bcaVq97ATaW0yAxk
http://love135.cjb.net/
http://&ltblocked>.cjb.net/

The first site contains an executable that the worm attempts to download and execute. This has been confirmed to be a backdoor Trojan, TROJ_BARIO.50. Barrio Trojan is mainly designed for collecting and sending passwords from the victim machine. It can collect dialup passwords, ICQ UIN and password, etc., and send them to a pre-defined e-mail address. The Trojan also deletes certain antivirus products installed in a system, and drops the files WTC.exe MixDaLaL.vbs, and Zacker.vbs. MixDaLaL.vbs is a Visual Basic Script file that is inserted in the \Windows\System folder. The Trojan/worm executes this file. As the file is executed, it will look through all folders on all fixed drives and network drives for files with the extensions .htm or .html. If such a file is found, they are overwritten with the message:

AmeRiCa ...Few Days WiLL Show You What We Can Do !!! I
It's Our Turn
>>> ZaCkEr is So Sorry For You

ZaCker.VBS is a file that is inserted in the \Windows\System folder. The Trojan/worm does not execute it. Instead, the value:

Norton.Thar \Windows\System\ZaCker.vbs

is added to the registry key:

HKEY_LOCAL_MACHINE\Microsoft\Windows\CurrentVersion\Run

so that the file is executed when you start Windows. When executed at the next restart, this file will attempt to delete all files in the \Windows folder. Next, the worm will create or overwrite the file C:\Autoexec.bat. Inside the file there will be a command that formats the C drive. The Autoexec.bat file is executed on Windows 95/98/Me and DOS systems when you start the computer. Finally, the following message is displayed:

I promiss We WiLL Rule The World Again…By The Way, You Are Captured By the ZaCker !!!

The worm does attempt to shut down Windows after the message has been displayed. However, because the files required for this event to occur have been deleted from the \Windows folder, the computer probably will not shut down.

TROJ_WHISTLER.A (Aliases: Whistler, WHISTLER.A): This Win32 Trojan appears as a Windows XP Serial Number Generator. It has been created in Visual C++ and carries a destructive payload of parsing drives and directories. Upon execution, the Trojan generates a fake Windows XP serial number and saves this number to a temporary file in the Windows temp directory. It then uses Notepad to open the file as it copies itself to a WHISTMNG.EXE file in the Windows System directory and creates the following run key in the registry so that it executes when the system is restarted:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run “Whistler” = “C:\<Systemdir>\whistmng.exe -next”

The Trojan then executes when the system is restarted and creates a WXP directory on the infected computer's Drive C:\ and parses directories and attempts to move every file that it finds to its created WXP directory. This includes moving the Windows System files to the WXP directory, which corrupts the system. This Trojan also recurses drives (local and mapped network drives). On drives that it parses after the Hard Drive C:\, it creates a ZWXP directory and not a WXP directory.

Trojan.ZeroBoot: This Trojan attempts to overwrites the boot sector of the hard disk with zeros. After the Trojan has executed, the computer will not boot from the hard drive.